

What Is Claimed Is:

1. A method for transmitting data (D), in which according to a specifiable signature formation method (SBV) a first signature (S) is formed as a function of the data (D) to be transmitted, the first signature (S) together with the data (D) is transmitted in so-called messages, a second signature (S') is formed according to the signature formation method as a function of the transmitted data (D') and the first signature (S) is compared with the second signature (S'),
wherein the data (D) to be transmitted are inverted, the first signature (S) is formed according to the specifiable signature formation method (SBV) as a function of the data (D) to be transmitted and of the inverted Data (D_i), the first signature (S) and the data (D) are transmitted, the transmitted data (D') are inverted, the second signature (S') is formed according to the signature formation method (SBV) as a function of these inverted data (D_i') and the transmitted data (D'), and the first signature (S) is compared with the second signature (S').
2. The method as recited in Claim 1,
wherein with the aid of a signature register (Sx) having multiple inputs (MISR; multiple input shift register) the first signature (S) and/or the second signature (S') are formed in a bit-parallel manner (word by word).
3. The method as recited in Claim 1 or 2,
wherein the first signature (S) and/or the second signature (S') are formed over several messages.
4. The method as recited in Claim 3,
wherein a signature (S) is transmitted by being distributed over several messages.
5. The method as recited in one of Claims 1 through 4, the data (D) to be transmitted being input data of a precision of one bit, which arrive at the processing units for example in messages via data buses, or calculation results, which are redundantly generated in parallel on multiple computers,
wherein for checking a match of these data (D) only the corresponding signatures (S) are transmitted.

6. The use of a method as recited in one of Claims 1 through 5, wherein the method according to the present invention is used for checking the content of a memory area of a read-only memory (21), flash memory or a read-write memory (22).
7. The use as recited in Claim 6, wherein the data (D) of the memory content to be verified are inverted, a first signature (S) is formed according to the specifiable signature formation method (SBV) as a function of the data (D) to be verified and of the inverted data (D_i) and is stored as a setpoint signature in a memory area of a read-only memory (21), flash memory or a read-write memory (22), and for verifying the data (D') located in the memory area to be verified, the data (D') are inverted and as a function of these inverted data (D_i') and of data (D') the second signature (S') is formed according to the signature formation method (SBV) and is compared with the setpoint signature(S).
8. A computer program executable on a computing unit or a control unit (SG1, SG2), in particular on a processing unit (RE1, RE2, RE3, RE4), wherein the computer program is suitable for carrying out a method as recited in one of Claims 1 through 5 when it runs on a processing unit (RE1, RE2, RE3, RE4).
9. The computer program as recited in Claim 8, wherein the computer program is stored on a memory element (20, 30), particularly on a random access read-write memory (RAM) (22, 32), a read-only memory (ROM) (21, 31) or a flash memory.
10. A control unit (SG1) for a motor vehicle, comprising at least one processing unit (RE1) and a memory element (20), on which a computer program is stored that is executable on the processing unit RE1, wherein the control unit (SG1) is suitable for carrying out a method as recited in one of Claims 1 through 5 when the computer program runs on the processing unit (RE1).